IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF OREGON

YOSHIDA FOODS INTERNATIONAL, LLC, an Oregon Limited Liability Company,

Plaintiff,

v.

FEDERAL INSURANCE COMPANY, an Indiana Corporation,

Defendant.

No. 3:21-cv-01455-HZ

OPINION & ORDER

Paul A. Mockford
Carson Riley
Parsons Farnell & Grein LLP
1030 SW Morrison Street
Portland, OR 97205

Attorneys for Plaintiff

Iga Wiktoria Todd
Scott Louis Schmookler
Gordon Rees Scully Mansukhani, LLP
1. N. Franklin, Ste 800
Chicago, IL 60606

Sally S. Kim
Gordon Rees Scully Mansukhani, LLP
701 5th Avenue, Ste 2100
Seattle, WA 98104

Attorneys for Defendant

HERNÁNDEZ, District Judge:

Plaintiff Yoshida Foods International, LLC ("Yoshida Foods") brings this action against Defendant Federal Insurance Company ("Federal") for breach of contract (Count One) and breach of the implied covenant of good faith (Count Two) because of Federal's denial of Plaintiff's insurance claim after it suffered a ransomware attack on March 29, 2021. Plaintiff seeks damages in the amount of $107,075.96 on Count One for Defendant's failure to pay the claim and $9,607.44 for actual and consequential damages on Count Two. Plaintiff moves for summary judgment on its breach of contract claim (Count One) and Defendant cross-moves for summary judgment on both counts.

For the reasons stated below, the Court grants Plaintiff's motion for summary judgment and denies Defendant's motion as to Count One. The Court grants summary judgment for Defendant on Count Two.

BACKGROUND

The relevant facts in this case are undisputed. Plaintiff Yoshida Foods is an Oregon limited liability company, whose sole owner/member is King Brewing Co., Ltd ("King Brewing"). Mockford Decl. Ex. 9, ECF 15-9. Yoshida Foods purchased insurance policy number 8260-3324 ("Policy"), effective October 1, 2020 to October 1, 2021, from Defendant Federal. Mockford Decl. Ex. 1, ECF 15-1. Included in the Crime Coverage Part of the Policy is "Section (E) Computer Fraud Coverage." *Id.* at 94. That section provides:

Insuring Clause (E): Computer Fraud Coverage

(E) The Company shall pay the **Parent Organization** for direct loss of **Money, Securities or Property** sustained by an **Insured** resulting from **Computer Fraud** committed by a **Third Party**.[1]

Id. at 96. Section (J) of the same part provides:

Insuring Clause (J): Expense Coverage

(J) The Company shall pay the **Parent Organization** for:

. . .

(2) **Computer Violation Expenses** resulting from any direct loss covered under Insuring Clauses (A), Employee Theft Coverage, (E), Computer Fraud Coverage, or (I), Client Coverage[.]

Id.

Section II of the Crime Coverage Part provides "Definitions" for relevant terms:

Computer Fraud means the unlawful taking of **Money, Securities** or **Property** resulting from a **Computer Violation**.

. . .

Computer Violation means an unauthorized:

(A) entry into or deletion of **Data** from a **Computer System**;

(B) change to **Data** elements or program logic of a **Computer System**, which is kept in machine readable format; or

(C) introduction of instructions, programmatic or otherwise, which propagate themselves through a **Computer System**,

directed solely against an **Organization**.

Computer Violation Expenses means reasonable expenses, other than an **Organization's** internal corporate costs (such as Salary), incurred by an **Organization** with the Company's prior written consent to reproduce or duplicate damaged or destroyed electronic **Data** or computer programs. If such programs cannot be duplicated from other computer programs, then Computer Violation Expenses shall also include reasonable costs incurred for computer time, computer programmers, technical experts or consultants to restore the computer program to substantially the same level of operational capability immediately preceding the covered direct loss.

Id. at 96-97.

[1] In the context of the Policy, "the Company" refers to Defendant Federal Insurance Company and "Parent Organization" refers to Plaintiff Yoshida Foods International, LLC.

Also included in the Crime Coverage Part of the Policy is Endorsement/Rider No. 8, effective October 1, 2020. Endorsement/Rider No. 8 provides a "Fraudulent Instructions Exclusion," which states:

> No coverage will be available under Insuring Clauses (B), (C), (D), (E), and (F) for loss resulting from any transfer, payment or delivery of **Money**, **Securities**, or **Property** approved by an **Employee** or arising out of any misrepresentation received by any **Employee**, agent, independent contractor or other representative of the Insured, whether such transfer, payment or delivery was made in good faith or as a result of trick, artifice, fraud or false pretenses.[2]

Id. at 120.

On March 29, 2021, an anonymous hacker gained unauthorized entry into Yoshida Foods' computer system and used malware to encrypt the data in the computer system's storage devices. Schaefer Decl. ¶ 3, ECF 13. The attack isolated and encrypted Yoshida Foods' entire network and all its data, rendering the system unusable. Mockford Decl. Ex. 10, ECF 15-10. Yoshida Foods' personnel discovered the attack when they arrived at work that morning and found that they could not access computer files. *Id.* When they tried to access the computer system, employees received a notification that the system was encrypted. *Id.* The notification included information on how to purchase decrypting programs that would restore access to the computer system and files. *Id.* In the notification, the hacker demanded a ransom payment of $25,000 in cryptocurrency in exchange for each decrypting program. *Id.* After seven days, according to the hacker, the price would double. *Id.*

Yoshida Foods sought assistance from its IT consultant, SharpForm Integration, Inc. ("SharpForm IT"), who concluded that the only way to recover access to the computer system

[2] Only Insuring Clause (E) covers Computer Fraud. Insuring Clauses (B), (C), (D), and (F) provide Premises Coverage, In Transit Coverage, Forgery Coverage, and Funds Transfer Fraud Coverage, respectively.

was to pay a $25,000 ransom for one decryption key. *Id.* at 2; Todd Decl. Ex. 1 ("Wand Dep.") 62:1-6, ECF 21-1. Yoshida Foods issued a check to SharpForm IT for $25,000, but SharpForm was unable to make the ransom payment in cryptocurrency. Mockford Decl. Ex. 11, ECF 15-11. Then, Yoshida Foods president, Junki Yoshida, and his financial advisor, Daniel McMorris, converted Mr. Yoshida's personal cryptocurrency funds into a form acceptable to the hacker for the ransom payment. Mockford Decl. Ex. 12, ECF 15-12. The payment was made from Mr. Yoshida's personal funds in consideration for future reimbursement by Yoshida Foods. *Id.*

The decryption key purchased from the hacker did not restore Yoshida Foods' computer system as SharpForm IT had hoped because backup hard drives failed and corrupted a substantial amount of data. Mockford Decl. Ex. 10. In order to fully restore all the data encrypted by the hacker, SharpForm IT had to purchase four decryption keys using Mr. Yoshida's cryptocurrency. *Id.* In total, by April 2, 2021, Mr. Yoshida had converted 197.14 Bitcoin Cash, valued at $107,074.20 to purchase the four decryption keys. Mockford Decl. Ex. 14, ECF 15-14. SharpForm IT then recovered all data and restored access to Yoshida Foods' computer system by April 5, 2021. Schaefer Decl. ¶ 7. Yoshida Foods paid SharpForm IT $7,075.96 for 62.25 hours of service that SharpForm provided between March 29, 2021 and April 9, 2021 to diagnose the source of the attack, acquire the decryption keys, recover data, and restore its computer system. Mockford Decl. Ex. 13, ECF 15-13.

After the ransomware attack and recovery of its computer system, Yoshida Foods filed a claim to Federal for reimbursement of $107,075.96 in expenses associated with the cyberattack under the Computer Fraud Coverage section of the Policy. Mockford Decl. Ex. 4, ECF 15-4. Yoshida Foods sought $100,000 for the ransom payment and $7,075.96 for reimbursement of its payment for SharpForm's IT services. *Id.* In a letter dated June 4, 2021, Federal informed

Yoshida Foods that it was denying the claim. *Id.* The letter explained that the ransom payment was not a "direct loss" to Yoshida Foods as required by Insuring Clause (E), the Computer Fraud Coverage section of the Policy. *Id.* at 3. The letter also stated that "there was no permanent loss of Money, Securities, or Property that directly resulted from a Computer Violation." *Id.* Federal further explained that the ransom payment was excluded under the Fraudulent Instructions Exclusion in the Policy. *Id.* Lastly, Federal denied coverage for the $7,075.96 Yoshida Foods paid to SharpForm IT because it erroneously determined that Yoshida Foods had not purchased such Expense Coverage as part of the Policy.[3] *Id.*

Prior to filing suit, Yoshida Foods' counsel conferred with Federal. Federal responded with a letter on July 15, 2021, again denying Plaintiff's claim. Mockford Decl. Ex. 5, ECF 15-5. In its second denial letter, Federal's explanation focused on the Fraudulent Instructions Exclusion. *Id.* Federal asserted that the exclusion applied because Mr. Yoshida was acting as an "Employee" of Yoshida Foods when he authorized the ransom payment. *Id.* Plaintiff filed this action on October 5, 2021, seeking coverage for its expenses under the Policy.

On May 27, 2022, one year after the ransomware attack, King Brewing, the sole member of Yoshida Foods, and Yoshida Management, LLC,[4] the manager of Yoshida Foods, officially approved the ransom payment made by Mr. Yoshida through a "Consent in Lieu of Special Meeting" agreement. Mockford Decl. Ex. 14. The agreement resolved "that the Manager is authorized and directed to cause [Yoshida Foods] to issue a reimbursement of the Ransom payment to Yoshida Management in the amount of $107,074.20." *Id.* On June 8, 2022, based on

[3] In the initial denial letter, Federal referred to the wrong policy when it determined that Yoshida Foods had not purchased Expense Coverage under Insuring Clause (J). Federal has since acknowledged this mistake but continues to assert that reimbursement for Plaintiff's IT expenses are unavailable under Insuring Clause (J).

[4] Junki Yoshida and Matthew Wand are the two managers of Yoshida Management, LLC.

the "Consent in Lieu of Special Meeting," Yoshida Foods Vice President Jill Sweeney instructed Jennifer Schmidt, account manager for Yoshida Foods, to transfer $107,074.20 to Yoshida Management. Solis Decl. ¶¶ 3, 4, ECF 21-2. On June 10, 2022, Yoshida Management then reimbursed Mr. Yoshida for that amount. *Id.* ¶¶ 5, 6.

STANDARDS

Summary judgment is appropriate if there is no genuine dispute as to any material fact and the moving party is entitled to judgment as a matter of law. Fed. R. Civ. P. 56(a). The moving party bears the initial responsibility of informing the court of the basis of its motion, and identifying those portions of "'the pleadings, depositions, answers to interrogatories, and admissions on file, together with the affidavits, if any,' which it believes demonstrate the absence of a genuine issue of material fact." *Celotex Corp. v. Catrett*, 477 U.S. 317, 323 (1986) (quoting former Fed. R. Civ. P. 56(c)).

Once the moving party meets its initial burden of demonstrating the absence of a genuine issue of material fact, the burden then shifts to the nonmoving party to present "specific facts" showing a "genuine issue for trial." *Fed. Trade Comm'n v. Stefanchik*, 559 F.3d 924, 927–28 (9th Cir. 2009) (internal quotation marks omitted). The nonmoving party must go beyond the pleadings and designate facts showing an issue for trial. *Bias v. Moynihan*, 508 F.3d 1212, 1218 (9th Cir. 2007) (citing *Celotex*, 477 U.S. at 324).

The substantive law governing a claim determines whether a fact is material. *Suever v. Connell*, 579 F.3d 1047, 1056 (9th Cir. 2009). The court draws inferences from the facts in the light most favorable to the nonmoving party. *Earl v. Nielsen Media Rsch., Inc.*, 658 F.3d 1108, 1112 (9th Cir. 2011). If the factual context makes the nonmoving party's claim as to the existence of a material issue of fact implausible, that party must come forward with more

persuasive evidence to support its claim than would otherwise be necessary. *Matsushita Elec. Indus. Co. v. Zenith Radio Corp.*, 475 U.S. 574, 587 (1986).

"Summary judgment is improper where divergent ultimate inferences may reasonably be drawn from the undisputed facts." *Fresno Motors, LLC v. Mercedes Benz USA, LLC*, 771 F.3d 1119, 1125 (9th Cir. 2014) (internal quotation marks omitted); *see also Int'l Union of Bricklayers & Allied Craftsman Loc. Union No. 20, AFL-CIO v. Martin Jaska, Inc.*, 752 F.2d 1401, 1405 (9th Cir. 1985) ("Even where the basic facts are stipulated, if the parties dispute what inferences should be drawn from them, summary judgment is improper.").

DISCUSSION

In its motion for summary judgment, Plaintiff asserts that its loss of more than $100,000 from the ransomware attack is covered under Insuring Clause (E), the Computer Fraud Coverage section of the Policy. Plaintiff argues that the ransomware was a "computer violation" that caused an "unlawful taking" of its money by requiring it to make a ransom payment. Plaintiff also asserts that the hackers engaged in an "unlawful taking" of its property by seizing and prohibiting access to its computer system. Plaintiff further argues that the Fraudulent Instructions Exclusion does not apply because "no 'Employee' of Yoshida Foods approved of the Ransom Payment." Pl. Mot. Summ. J. 19, ECF 12. Finally, Plaintiff contends that Insuring Clause (J) authorizes reimbursement for the $7,075.96 it paid for IT services to restore its computer system after the attack.

In its cross-motion for summary judgment, Defendant asserts that Plaintiff did not suffer a "direct loss" from computer fraud. According to Defendant, the only loss Plaintiff suffered was when it reimbursed Mr. Yoshida for the ransom payment he made with his own cryptocurrency. Defendant notes that Mr. Yoshida is not personally insured under the Policy.

Defendant also contends that the Fraudulent Instructions Exclusion bars coverage because Ms. Schmidt, the account manager, "approved the transfer in that she formally authorized it on behalf of Yoshida Foods." Def. Mot. Summ. J. 10, ECF 20. In the alternative, Defendant argues that Mr. Yoshida was acting as an "Employee" when he approved the ransom payment. Defendant further argues that the IT service expenses Plaintiff incurred are not covered under Insuring Clause (J). Defendant notes that Insuring Clause (J) only applies when there is a direct loss under the Computer Fraud Coverage section and asserts that any covered IT expenses would have required the insurance company's prior written consent.

I. Insurance Contract Interpretation

Under Oregon law, interpreting the terms and conditions of an insurance policy is a matter of law for the court. *Bresee Homes, Inc. v. Farmers Ins. Exch.*, 227 Or. App. 587, 590, 206 P.3d 1091, 1093 (2009), *rev'd on other grounds*, 353 Or. 112, 293 P.3d 1036 (2012). A court must determine the parties' intent by examining the specific terms of the policy. *Hoffman Const. Co. of Alaska v. Fred S. James & Co. of Oregon*, 313 Or. 464, 469, 836 P.2d 703, 706 (1992). "In interpreting an insurance policy, we seek to ascertain the intent of the parties as interpreted from the perspective of the 'ordinary purchaser of insurance.'" *Capitol Specialty Ins. Corp. v. Chan & Lui, Inc.*, 248 Or. App. 674, 680, 274 P.3d 238, 240 (2012) (quoting *Totten v. New York Like Ins. Co.*, 298 Or. 765, 771, 696 P.2d 1082 (1985).

A court first examines the text of the policy to determine whether it is susceptible to more than one plausible interpretation. *Andres v. Am. Standard Ins. Co.*, 205 Or. App. 419, 423, 134 P.3d 1061 (2006). If the text is not ambiguous, "the policy is interpreted in accordance with that unambiguous meaning." *Id.* If the text of an insurance policy is susceptible to more than one

interpretation, any doubt as to the meaning of the text is interpreted against the insurer. *Id*. at 240-241.

Insuring Clause (E), the Crime Fraud coverage provision of the Policy, contains several terms that are subject to interpretation. The Clause provides that Defendant "shall pay [Plaintiff] for direct loss of Money, Securities or Property sustained by [Plaintiff] resulting from Computer Fraud committed by a Third Party." Mockford Decl. Ex. 1. The Policy defines "Computer Fraud" as "the unlawful taking of Money, Securities or Property resulting from a Computer Violation. *Id.* at 96. A "Computer Violation" includes, among other acts, "entry into or deletion of Data from a Computer System," and "introduction of instructions, programmatic or otherwise, which propagate themselves through a Computer System." *Id.* at 97.

The parties disagree about the meaning of "Computer Fraud" and "Computer Violation" as defined by the Policy. But Defendant does not specifically argue that the ransomware attack was not computer fraud or a computer violation and does not base its denial of coverage on the meaning of those terms. Rather, Defendant asserts that coverage is unavailable under Insuring Clause (E) because Plaintiff did not sustain a "direct loss" from the ransomware attack.

II. "Direct Loss" Under Insuring Clause (E)

According to Defendant, Plaintiff suffered no loss because it did not make the ransom payment—Mr. Yoshida did. Mr. Yoshida is not personally covered for his loss under the Policy. Defendant claims that the only loss incurred by Plaintiff was its reimbursement to Mr. Yoshida, more than one year after the ransomware attack. Defendant asserts that Plaintiff's reimbursement for the ransom payment was an indirect or consequential loss to Plaintiff rather than a direct loss due to the computer violation.

The Policy does not define "direct loss." The word "direct" means "characterized by or giving evidence of a close esp. logical, causal, or consequential relationship*." Papi, LLC v. Cincinnati Ins. Co.*, 3:21-cv-00405-JR, 2021 WL 6932657, at *4 (D. Or. Nov. 10, 2021), findings and recommendation adopted, 2022 WL 475910 (D. Or. Feb. 16, 2022) (quoting Webster's Third New Int'l Dictionary 640 (unabridged ed. 2002)). Courts have interpreted "direct" in the context of insurance coverage to mean "without any intervening agency or step: without any intruding or diverting factor." *Whitney Equip. Co., Inc. v. Travelers Cas. & Sur. Co. of Am.*, 431 F. Supp. 3d 1223, 1228 (W.D. Wash. 2020). Thus, "direct" refers to "the necessary causal relationship, namely a cause which in a direct sequence, unbroken by any independent cause, produced the injury complained of and without which such injury would not have happened." *Id.* at 1229 (internal quotation and citation omitted). Oregon courts have held that "direct loss" describes "a proximate, rather than remote, relationship" between the act covered under the policy and the resulting loss or damage. *Summit Real Est. Mgmt., LLC v. Mid-Century Ins. Co.*, 298 Or. App. 164, 177, 445 P.3d 905, 912 (2019).

In claiming that Plaintiff's loss from the ransomware attack was not "direct," Defendant relies on a district court's holding in *Taylor & Lieberman v. Federal Insurance Co.*, No. CV 14-3608 RSWL (SHx), 2015 WL 3824130 (C.D. Cal. June 18, 2015), *aff'd*, 681 F. App'x 627 (9th Cir. 2017). In *Taylor*, Federal Insurance Company denied coverage to the plaintiff, an accounting corporation, under a Computer Fraud provision like the one at issue here. *Id.* at *4. In that case, employees of the plaintiff were induced by fraudulent emails to transfer funds from a client's account to a third party. *Id.* The plaintiff sought reimbursement from the insurance company for its repayment to the client of the amount of money lost through the fraudulent transfer. *Id.* The district court denied relief for the plaintiff, holding that "the e-mails did not immediately and

without intervening cause result in a loss" because the plaintiff's loss only occurred after it failed to recover the funds and the client demanded repayment. *Id.* at *3. According to the court, "a loss is not direct unless it follows immediately and without intervening space, time, agency, or instrumentality." *Id.*

The Ninth Circuit affirmed the district court's holding on other grounds. *Taylor*, 681 F. App'x at 628. Without discussing the district courts rationale, the Ninth Circuit found that computer fraud coverage was unavailable under the policy because there was no unauthorized "entry into" the plaintiff's computer system. *Id.* at 629. The plain meaning of the policy required a virus or introduction of malicious code for computer fraud coverage to apply. *Id.* In so holding, the Ninth Circuit did not address whether the plaintiff had suffered a "direct loss."

Importantly, *Taylor* was not a case about ransomware. Here, unlike in *Taylo*r, the hacker entered into Plaintiff's computer system and installed malware that encrypted and froze the system and data files. Thus, the Ninth Circuit's reason for affirming Federal's denial of coverage does not apply to this case. And under Oregon courts' interpretation of "direct loss," only a proximate causal relationship is necessary. *See Summit Real Est. Mgmt., LLC*, 298 Or. App. at 177.

Both the ransom payment made by Mr. Yoshida and the reimbursement of that amount by Plaintiff were proximately caused by the hacker's computer violation directed against Plaintiff's computer system. There was no intervening occurrence between the ransomware attack, the ransom payment, and the reimbursement to Mr. Yoshida, which were all part of an unbroken sequence of events. Plaintiff's reimbursement of the $107,074.20 ransom payment was a foreseeable result of the attack. *See Whitney Equip.*, 431 F. Supp. 3d at 1229 (holding that the

insured suffered a direct loss when the insurer "failed to show any intervening agency or occurrence: the entire course of events was entirely foreseeable[.]").

The Court also finds that whether Plaintiff's loss occurred when Mr. Yoshida made the ransom payment or when Plaintiff reimbursed Mr. Yoshida is irrelevant. Regardless of when the loss occurred, Plaintiff's loss was a direct result of the ransomware attack. Mr. Yoshida made the payment from his personal funds because Plaintiff had no capacity to directly pay the ransom in cryptocurrency, the form of payment required by the hacker. Even if Plaintiff's loss actually occurred one year later when it reimbursed Mr. Yoshida, the loss was still a direct and foreseeable consequence of the computer fraud perpetrated by the hacker. The passage of time did not break the causal chain because there was always an understanding that the ransom payment was a liability to Plaintiff, not to Mr. Yoshida personally. Thus, that the payment to the hacker came from Mr. Yoshida's personal funds does not preclude a finding that Plaintiff suffered a direct loss.

Defendant next argues that because Plaintiff "made a conscious decision to pay a cyber-criminal . . . that payment was not a direct result of the Computer Violation." Def. Mot. Summ. J. 21. Defendant essentially argues that Plaintiff could only suffer a "direct" loss if the hacker had hacked into the computer system and had directly stolen funds without Plaintiff's involvement. In making this argument, Defendant relies on *Pestmaster Services, Inc. v. Travelers Casualty and Surety Company of America*, No. CV 13-5039-JFW (MRWx), 2014 WL 3844627, *aff'd* in part, *vacated* in part, 65 F. App'x 332 (9th Cir. 2016). In *Pestmaster*, a company the plaintiff had hired to perform payroll tax services perpetrated a fraudulent scheme against the plaintiff. *Id.* at *1-2. The plaintiff expressly authorized the fraudulent electronic payments to the company. *Id.* The district court found that a Funds Transfer Fraud provision of the insurance policy "[did] not

cover authorized or valid electronic transfers . . . even though they are, or may be, associated with a fraudulent scheme." *Id.* at *5. But the court found no coverage under the Computer Crime provision for a different reason—"the transfer of funds . . . did not involve hacking or any unauthorized entry into a computer system." *Id.* at *7. The court also found that the use of a computer in the fraudulent scheme "was merely incidental to, and not directly related to" the plaintiff's loss of funds. *Id.* Thus, *Pestmaster* presents a very different set of circumstances than this case. Here, the hacker's entry into Plaintiff's computer system was central to the scheme to extort money from Plaintiff.

In affirming, the Ninth Circuit "interpret[ed] the phrase fraudulently cause a transfer to require an *unauthorized* transfer of funds." *Pestmaste*r, 65 F. App'x at 333 (emphasis added). But in so holding, the Ninth Circuit was referring to a computer being used as an instrument to transfer funds. The court explained that "[b]ecause computers are used in almost every business transaction, reading this provision to cover all transfers that involve both a computer and fraud at some point in the transaction would convert this Crime Policy into a "General Fraud" Policy." *Id.* But *Pestmaster* did not involve a hacker's entry into a computer system and demand for a ransom payment. Thus, the alleged fraud in ***Pestmaster*** was not due to a "computer violation" and is distinguishable from the computer fraud alleged in this case — a ransomware attack.

In a more recent case, the Ninth Circuit reversed a district court decision in favor of an insurance company because the district court improperly relied on the holding in *Pestmaste*r. *Ernst and Haas Mgmt. Co., Inc. v. Hiscox, Inc.*, 23 F. 4th 1195, 1199-1200 (9th Cir. 2022). In *Ernst*, a property management company sought insurance coverage under a computer fraud provision after fraudulent emails induced an employee to transfer $200,000 to a "swindling third party." *Id.* at 1196-97. The defendant insurance company claimed that coverage was unavailable

because the employee had "taken action to initiate a wire transfer." *Id.* at 1197. The district court granted the defendant's motion to dismiss, holding that the plaintiff's loss did not result directly from fraudulent emails. *Id.* at 1199. The district court interpreted the computer fraud provision to mean a direct loss is limited to unauthorized use of a computer, such as a hacker entering a computer system to initiate a transfer and steal funds. *Id.* at 1200. The district court found that the employee's volitional transfer precluded a finding of direct loss from computer fraud.

In reversing, the Ninth Circuit held that "initiating a wire transfer is not the same as authorizing a payment." *Id.* at 1200. The court noted that a volitional payment induced by fraud is, by definition, not authorized. *Id.* According to the Ninth Circuit, "[t]hat reasoning—that this fraud became "authorized" precisely when it succeeded—cannot be the correct reading of the contract." *Id.* at 1201.

Here, the computer fraud is even more directly related to the loss than in *Ernst*. Unlike in *Ernst*, the perpetrator did hack into Plaintiff's computer system. Although the hacker did not manipulate the computer system to initiate the transfer herself, the hacker encrypted the system so that Plaintiff could not use it and demanded a ransom payment. The ransom payment was a direct loss to Plaintiff. Plaintiff's volitional payment does not negate the fact that Plaintiff suffered a direct loss due to a computer violation.

A recent case decided by the Supreme Court of Indiana addressed whether a ransom payment after a cyberattack is a "direct loss" under a computer fraud insurance policy. *G&G Oil Co. of Indiana v. Cont'l W. Ins. Co.*, 165 N.E.3d 82 (Ind. 2021). In that case, hackers gained access to the plaintiff G&G Oil's computer system and froze its servers. *Id.* at 85. After consulting experts, G&G Oil negotiated with the hackers and ultimately paid $35,000 in bitcoins to regain access to the computer systems. *Id.* at 85. The defendant insurance company denied

G&G Oil's claim under the computer fraud provision of the insurance policy. *Id.* at 86. The court summarized the parties' contentions:

> G&G Oil contends its loss resulted directly from the use of a computer under the terms of the Policy because a computer was part and parcel of the entire scheme. Continental argues, and the trial court concluded, that G&G Oil's voluntary transfer of Bitcoin was an intervening cause that severed the causal chain of events.

Id. at 90.

Even though the hacker did not directly initiate the transfer of funds and the plaintiff had made the payment volitionally, the court in *G&G Oil* held in favor of the plaintiff. The court reasoned:

> Analyzing G&G Oil's actions in this case, its transfer of Bitcoin was nearly the immediate result—without significant deviation—from the use of a computer. Though certainly G&G Oil's transfer was voluntary, it was made only after consulting with the FBI and other computer tech services. The designated evidence indicates G&G Oil's operations were shut down, and without access to its computer files, it is reasonable to assume G&G Oil would have incurred even greater loss to its business and profitability. These payments were "voluntary" only in the sense G&G Oil consciously made the payment. To us, however, the payment more closely resembled one made under duress. Under those circumstances, the "voluntary" payment was not so remote that it broke the causal chain. Therefore, we find that G&G Oil's losses "resulted directly from the use of a computer."

Id. at 90-91.

While the holding in *G&G Oil* is not binding, the Court finds its reasoning persuasive. As in that case, Plaintiff suffered a ransomware attack that froze its computer system. The hacker required payment in cryptocurrency, which Plaintiff made volitionally but under duress. Had Plaintiff not made the payment, its entire computer system would have remained nonfunctional, resulting in even greater loss. Thus, Plaintiff's coerced decision to make the ransom payment cannot be considered voluntary. And the hacker's requirement for payment in cryptocurrency forced Plaintiff to immediately turn to Mr. Yoshida to lend funds for the payment. As in *G&G*

Oil, the Court finds that Plaintiff's reimbursement to Mr. Yoshida for the ransom payment was not so remote that it broke the causal chain resulting in a direct loss from computer fraud.

III. Fraudulent Instructions Exclusion

Endorsement/Rider No. 8, the Fraudulent Instructions Exclusion, provides that no coverage is available under the Computer Fraud Coverage section of the Policy for any transfer or payment of money "approved" by an "employee" of the insured. Defendant argues that the Fraudulent Instructions Exclusion applies because the payment for which Plaintiff seeks insurance coverage was "formally authorized" by Jennifer Schmidt, Plaintiff's accounting manager. Alternatively, Defendant asserts that if the payment at issue was the cryptocurrency transfer made by Mr. Yoshida, the exclusion applies because Mr. Yoshida was acting as an employee when he authorized payment to the hacker. Defendant's arguments are unavailing.

First, Defendant contends that Ms. Schmidt's clerical task of processing the reimbursement payment to Mr. Yoshida was an official "approval" of a transfer of funds. The plain language of the Fraudulent Instructions Exclusion suggests that its purpose is to prohibit reimbursement when an employee erroneously responds to a fishing email or complies with an email that provides fraudulent instructions to transfer funds. Ms. Schmidt did not erroneously authorize the reimbursement payment. Nor did she make the payment on her own accord. Rather, she simply processed a reimbursement payment from Plaintiff to Yoshida Management, LLC (who then reimbursed Mr. Yoshida) that was authorized by Plaintiff's sole member, King Brewing. Thus, as to Ms. Schmidt's processing of the reimbursement payment, the Fraudulent Instructions Exclusion does not apply.

As to Mr. Yoshida's payment of cryptocurrency for the ransom, the exclusion also does not apply. The parties disagree about whether Mr. Yoshida acted as an "employee" when he

authorized the ransom payment. Defendant asserts that Mr. Yoshida is a "a W-2 employee of Yoshida Foods International." Wand Dep. 24:6-7. Plaintiff argues that Mr. Yoshida is not an "employee" as defined by the Policy because, as the president of Yoshida Foods, he is an executive. The definition of "employee" in the Crime Coverage part of the Policy includes the following relevant sections:

> Employee means any:
>
> (A) natural person in the regular service of an **Organization** in the ordinary course of such **Organization's** business, whom such **Organization** governs and directs in the performance of such service, including a part-time, seasonal, leased and temporary employee, intern or volunteer; [or]
> (B) **Executive** while performing acts within the scope of the usual duties of an **Employee**[.]

Mockford Decl. Ex. 1, at 97.

Defendant argues that Mr. Yoshida is an "employee" because he is in the regular service of Yoshida foods, who governs and directs the performance of his service. Alternatively, Defendant asserts that even if Mr. Yoshida is an "executive," he met the Policy definition of "employee" because when he made the ransom payment, he acted as an employee. Defendant notes that courts have found that approval of transactions and payments falls within the scope of the usual duties of an employee. *See Puget Sound Nat. Bank v. St. Paul Fire and Marine Ins. Co.*, 32 Wash. App. 32, 39, 645 P.2d 1122, 1126 (1982).

But Mr. Yoshida's decision to pay the cryptocurrency ransom could not have been made by an ordinary employee in the usual course of performing their duties. The ransomware attack was an extraordinary situation, which required a decision to be made by Mr. Yoshida as an executive of the company to regain control of its computer system. In addition, a typical employee would not pay $100,000 of their personal money in the usual course of their duties as an employee. Finally, that Mr. Yoshida's payment was later "confirmed, ratified, and approved

in all respects" by King Brewing and Yoshida Management shows that paying the ransom was a high-level decision, which would not fall within the scope of the usual duties of an employee. Mockford Decl. Ex. 14.

The parties also disagree about whether the Fraudulent Instructions Exclusion applies to transfers or payment compelled under duress. The specific language of that section excludes transfers approved by employees whether the transfer "was made in good faith or as a result of trick, artifice, fraud or false pretenses." Mockford Decl. Ex. 1, at 120. Plaintiff argues that Mr. Yoshida did not "approve" the ransomware payment because he was coerced into making the payment. Defendant counters by contending that the Fraudulent Instructions Exclusion applies to all authorized payments by employees, even if those payments are induced by crime. *See Aqua Star (USA) Corp. v. Travelers Cas. & Sur. Co. of Am.*, No. C14-1368RSL, 2016 WL 3655265, at *1 (W.D. Wash. July 8, 2016) (finding a coverage exclusion applied when employees were induced by fraudulent emails to initiate fraudulent transfers to third parties); *but see G&G Oil*, 165 N.E.3d at 90 (holding that volitional payments made under duress were not voluntarily approved by employees). Under Defendant's reading, if someone held a gun to an employee's head demanding payment, and the employee made the payment, the act of paying would have been "approved" by the employee. And according to Defendant, the ransom payment made by Mr. Yoshida under similar duress was "approved" by him. The Court does not agree.

As described in II., *supra*, the Court finds the Indiana Supreme Court's reasoning in *G&G Oil* to be persuasive. Thus, even if Mr. Yoshida had acted as an employee, he did not "approve" of the ransom payment needed for Plaintiff to regain access to its computer system because the payment was coerced. As to both Mr. Yoshida's payment of the cryptocurrency

ransom and Ms. Schmidt's processing of Plaintiff's reimbursement to Mr. Yoshida, the Fraudulent Instructions Exclusion does not apply.

IV. Insuring Clause (J) for "Computer Violation Expenses"

Along with insurance coverage for the ransom payment, Plaintiff seeks reimbursement of $7,075.96 for its payment to SharpForm IT for the 62.25 hours of service SharpForm provided in restoring Plaintiff's access to its computer system. Defendant notes that coverage under Insuring Clause (J) for "Computer Violation Expenses only applies to costs "resulting from any *direct loss* covered under Insuring Clause . . . (E), Computer Fraud Coverage[.]" Mockford Decl. Ex. 1 at 96 (emphasis added). Defendant argues that Insuring Clause (J) does not cover Plaintiff's IT expenses because Plaintiff did not suffer a "direct loss." The Court finds that Plaintiff suffered a direct loss from the ransomware attack. *See* II., *supra*. Thus, coverage under Insuring Clause (J) is not barred for this reason.

Defendant also argues that Insuring Clause (J) only covers expenses that Plaintiff incurred after receiving Defendant's prior written consent. The Policy defines Computer Violation Expenses as:

> reasonable expenses . . . incurred by an Organization with the Company's *prior written consent* to reproduce or duplicate damaged or destroyed electronic Data or computer programs. If such programs cannot be duplicated from other computer programs, then Computer Violation Expenses shall also include reasonable costs incurred for computer time, computer programs, technical experts or consultants to restore the computer programs to substantially the same level of operational capability immediately preceding the covered direct loss.

Id. at 97 (emphasis added).

Reading the definition literally, a Computer Violation Expense requires prior written consent only for the cost to reproduce or duplicate damaged or destroyed electronic data or computer programs. But the second sentence of the definition, which applies"[i]f such programs

cannot be duplicated," does not include a requirement for prior written consent for costs associated with restoring computer programs. SharpForm IT did not reproduce or duplicate damaged or destroyed electronic data. Rather, SharpForm IT determined that Plaintiff's computer programs could not be reproduced because the hacker's malware encrypted data on Plaintiff's backup hard drives as well as its computer storage devices. Schaefer Decl. ¶¶ 3, 5.

Based on the plain language of Insuring Clause (J), no prior written consent was required for Plaintiff to recover the cost of services rendered by SharpForm IT to diagnose and restore access to its computer system and files.[5] At minimum, the Policy is ambiguous as to whether prior consent is needed for the computer restoration expenses Plaintiff incurred. And under Oregon law, any ambiguity in an insurance contract is construed against the insurer. *Capitol Specialty Ins. Co.*, 248 Or. App. at 240-241. Thus, the Court finds that Insuring Clause (J) covers the $7,075.96 that Plaintiff paid SharpForm IT to restore its computer system after the ransomware attack.[6]

V. Breach of the Duty of Good Faith and Fair Dealing

In Count Two of its claim seeking insurance coverage, Plaintiff alleges Defendant breached an implied duty of good faith and fair dealing under the insurance contract. Defendant moves for summary judgment on Count Two, but Plaintiff does not.

[5] According to SharpForm IT's invoice for its services, it spent 62.25 hours to "Diagnose source of attack"; "Re-install the operating system on all affected desktop computers to remove malware"; "Acquire decryption key tools to decrypt servers so they can be restored from backup"; and "Complete decryption of required data." Mockford Decl. Ex. 13, ECF 15-13.

[6] Defendant contends that the $7,075.96 in computer violation expenses incurred by Plaintiff "does not exceed the $10,000 Retention applicable to Insuring Clause (E)." Def. Mot. Summ. J. 22, ECF 20. But Plaintiff seeks to recover this amount under Insuring Clause (J), which covers costs up to $100,000 without a minimum retention amount. Mockford Decl. Ex. 1, at 94.

Under Oregon law, parties to a contract have a good faith obligation "to perform the contract, including exercising any discretion that the contract provides, in a way that will effectuate the objectively reasonable contractual expectations of the parties." *Veloz v. Foremost Ins. Co. Grand Rapids, Mich.*, 306 F. Supp. 3d 1271, 1280 (D. Or. 2018) (quoting *Pollock v. D.R. Horton, Inc.—Portland*, 190 Or. App. 1, 77 P.3d 1120, 1127 (2003)). Although related, claims for breach of an implied covenant of good faith are distinct from breach of contract claims. *Foraker v. USAA Cas. Ins. Co.*, 345 F. Supp. 1308, 1310 (D. Or. 2018). Every successful breach of contract claim is not necessarily a per se breach of the duty of good faith. *Veloz,* 306 F. Supp. at 1281. When an insurer adopts a "plausible yet ultimately incorrect reading of the contract language . . . a breach of the duty of good faith claim requires evidence of something beyond the mere breach of contract to proceed." *Id.*

Plaintiff alleges that Defendant breached its contractual duty to act in good faith by "applying unreasonable and arbitrary interpretations of [the] Policy to deny the Claim." Compl. ¶ 24. Plaintiff agrees that the standard for determining good faith in denying insurance coverage is reasonableness. But Plaintiff claims that Defendant's decision to deny coverage for the ransomware payment was unreasonable.

In explaining why it believes Defendant's denial was unreasonable and not in good faith, Plaintiff rehashes its arguments as to why its loss from the ransomware attack is covered under the Policy. Plaintiff adequately shows why its interpretation of the Policy terms is more persuasive than that of Defendant. But Plaintiff presents no evidence that Defendant acted dishonestly, with reckless disregard, or without any reasonable basis for denying Plaintiff's claim. As this court in *Veloz* explained,

> [t]here likely are cases where an insurer's interpretation of policy language is so patently unreasonable that denial alone could support a breach of good faith claim,

> but that is because an insurer's adoption of a truly beyond-the-pale interpretation of contractual language is evidence that the insurer was willing to disregard the objectively reasonable contractual expectations of the insured.

Id. at 1281.

The Computer Fraud Coverage provision of the Policy does not include the words "ransomware" or "encryption." Although that provision expressly covers a direct loss from a computer violation, the language in the insurance contract is not specifically tailored to a ransomware attack such as the one experienced by Plaintiff. Accordingly, whether the Policy provides coverage for such an attack is subject to interpretation and disagreement. The Court finds that the Policy does cover Plaintiff's ransom payment and IT expenses. But the Court finds no indication that Defendant's contrary interpretation lacked good faith. Like the defendant insurance company in *Veloz*, Defendant "adopted a plausible yet ultimately incorrect reading of the contract language." *Id.* And "[u]nder those circumstances, a breach of the duty of good faith claim requires evidence of something beyond the mere breach of contract to proceed." *Id.* Plaintiff provides no such evidence. That Defendant breached its contract with Plaintiff is insufficient to show that Defendant breached its duty of good faith. Thus, Defendant is entitled to summary judgment on Plaintiff's good faith claim.

///

///

///

///

///

///

///

CONCLUSION

For the reasons stated above, the Court GRANTS Plaintiff's Motion for Summary Judgment [12] and GRANTS in part and DENIES in part Defendant's Motion for Summary Judgment [20]. The Court GRANTS summary judgment for Plaintiff on its claim for breach of contract and GRANTS summary judgment for Defendant on Plaintiff's claim for breach of an implied covenant of good faith and fair dealing.

IT IS SO ORDERED.

DATED: December 6, 2022.

MARCO A. HERNÁNDEZ
United States District Judge